Защита объектов критической инфраструктуры

написано GlobalTrust.ru | 20.08.2023

Обеспечение безопасности критической информационной инфраструктуры Российской Федерации

GlobalTrust реализует полный комплекс мероприятий по разработке Системы обеспечения безопасности объектов Ключевой информационной инфраструктуры (СОБ ОКИИ) в соответствии с требованиями 187-ФЗ «О безопасности критической информационной инфраструктуры РФ» и нормативными документами РФ в области защиты информации.

С 1 января 2018 года вступил в силу **Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»**. Закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении нее компьютерных атак.

Закон распространяется на субъекты КИИ – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальных предпринимателей, которым по праву собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере: здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, атомной энергии, оборонной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности, химической промышленности.

В соответствии с Законом безопасность КИИ обеспечивается за счет:

- Категорирования объектов КИИ в соответствии с установленными Правительством РФ показателями критериев значимости объектов КИИ и их значений
- Ведения реестров объектов КИИ с учетом их категории опасности
- Установления требований к системам безопасности объектов КИИ с учетом их категории опасности
- Обеспечения взаимодействия этих систем с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)
- Осуществления анализа защищенности КИИ и ее объектов
- Осуществления государственного контроля в области безопасности КИИ

Система обеспечения безопасности КИИ

Для приведения в соответствие требованиям 187-ФЗ субъектам КИИ необходимо провести мероприятия по категорированию объектов КИИ, а также разработать и внедрить Систему обеспечения безопасности объектов Ключевой информационной инфраструктуры (СОБ ОКИИ), которая представляет собой комплекс программно-технических средств, а также организационно-технических мероприятий, направленных на предотвращение, ликвидацию угроз или на минимизацию ущерба от реализации угроз безопасности в отношении объектов КИИ.

В состав СОБ ОКИИ входят следующие основные программно-технические подсистемы:

- Подсистема управления доступом
- Подсистема регистрации и учета
- Подсистема обеспечения целостности
- Подсистема антивирусной защиты
- Подсистема анализа защищенности
- Подсистема обнаружения вторжений

- Подсистема межсетевого экранирования

Управление СОБ ОКИИ осуществляется путем документирования и реализации следующих основных процессов:

- Планирование СОБ ОКИИ
- Реагирование на инциденты (нарушения) безопасности информации в объекте КИИ
- Оценка рисков реализации угроз деструктивных информационных воздействий на объект КИИ
- Защита носителей информации
- Обеспечение целостности программно-аппаратной среды объекта КИИ
- Физическая защита объекта КИИ и среды ее функционирования
- Управление персоналом объекта КИИ
- Информирование и обучение персонала по вопросам СОБ ОКИИ
- Защита коммуникаций
- Аудит безопасности информации

Разработка СОБ ОКИИ осуществляется в соответствии с требованиями действующего законодательства, ГОСТов и нормативной базы РФ в области защиты информации.

Этапы разработки системы обеспечения безопасности КИИ

Этапы разработки СОБ ОКИИ включают в себя следующее:

1. Предпроектный этап
2. Проектирование СОБ ОКИИ
3. Разработка организационно-распорядительных документов по СОБИ ОКИИ
4. Ввод в действие

Предпроектный этап

Предпроектный этап, включает в себя предпроектное обследование объекта КИИ (или территории, помещений организации, где предполагается развернуть объект КИИ), разработку аналитического обоснования необходимости создания СОБ ОКИИ и ТЗ (ЧТЗ) на ее создание.

Предпроектное обследование

На предпроектном этапе определяется:

- Конфигурация и топология объекта КИИ, используемых систем связи и их отдельных компонентов, функциональные и технологические связи как внутри объекта КИИ, так и с другими системами различного уровня и назначения
- Состав и содержание критически важной информации применительно к данному объекту КИИ
- Аппаратные и программные средства объекта КИИ, используемые для обработки, хранения, передачи и приема критически важной информации и режимы ее обработки
- Степень участия должностных лиц организации в обработке (обсуждении, передаче, хранении) критически важной информации, характер их взаимодействия между собой и со службой безопасности
- Угрозы безопасности информации, связанные с НСД к защищаемой критически важной информации и несанкционированными воздействиями на нее, формируется модель вероятного нарушителя применительно к конкретным условиям функционирования объекта КИИ
- Мероприятия по обеспечению конфиденциальности критически важной информации об объекте КИИ на этапе проектирования и создания СОБ ОКИИ

Разработка аналитического обоснования

По результатам предпроектного обследования объекта КИИ составляется аналитическое обоснование необходимости создания СОБ ОКИИ, которое содержит:

- Информационную характеристику и организационную структуру объекта КИИ
- Характеристику комплекса основных и вспомогательных технических средств, программного обеспечения, режимов работы объекта КИИ, процесса обработки информации
- Описание возможных каналов деструктивных информационных воздействий на объект КИИ, каналов утечки (разглашения) критически важной информации об объекте КИИ и характеристику мероприятий по их устранению и ограничению
- Перечень предлагаемых к использованию сертифицированных СЗИ
- Обоснование необходимости привлечения для создания СОБ ОКИИ специализированных организаций, имеющих необходимые лицензии на право проведения работ по защите информации
- Оценку материальных, трудовых и финансовых затрат на разработку и внедрение СОБ ОКИИ
- Ориентировочные сроки разработки и внедрения СОБ ОКИИ
- Перечень мероприятий по обеспечению конфиденциальности критически важной информации об объекте КИИ на этапе проектирования и создания СОБ ОКИИ

Разработка технического задания

По результатам предпроектного обследования составляется ТЗ на разработку СОБ ОКИИ в соответствии с ГОСТом Р 51583-2000 «Защита информации. Порядок создания автоматизированной системы в защищенном исполнении. Общие требования» и ГОСТом 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированную систему. Техническое задание на создание автоматизированной системы».

Техническое задание на разработку СОБ ОКИИ содержит:

- Обоснование разработки СОБ ОКИИ
- Исходные данные об объекте КИИ в техническом, программном, информационном и организационных аспектах
- Уровень значимости объекте КИИ
- Требования по обеспечению безопасности, предъявляемые к объекту КИИ

- Перечень предполагаемых к использованию сертифицированных СЗИ
- Обоснование проведения разработок собственных СЗИ, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных СЗИ
- Состав, содержание и сроки проведения работ по этапам разработки и внедрения СОБ ОКИИ
- Перечень подрядных организаций — исполнителей видов работ
- Перечень предъявляемой заказчику научно-технической продукции и документации

Этап техно-рабочего проектирования

На этапе проектирования осуществляется разработка проектных решений по СОБ ОКИИ и её частям, на основе которых создаются следующие основные проектные документы:

- Техно-рабочий проект СОБ ОКИИ в соответствии с ГОСТом 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированную систему. Виды, комплектность и обозначение документов при создании автоматизированной системы»
- Эксплуатационная документация, включающая в себя технический паспорт на СОБ ОКИИ, а также инструкции и руководства по эксплуатации технических и программных средств СОБ ОКИИ для пользователей, администраторов системы и сотрудников службы безопасности

Этап разработки организационно-распорядительной документации

На следующем этапе осуществляется разработка комплекса внутренних организационно-распорядительных документов по СОБ ОКИИ, включающего в себя следующее:

- Положение об обеспечении безопасности объекта КИИ
- План обеспечения безопасности объекта КИИ

- Правила поведения сотрудников в отношении СОБ ОКИИ
- План действий в непредвиденных ситуациях
- Положение об управлении инцидентами и процедуры реагирования на инциденты
- Положение об управлении информационными рисками
- Методика оценки информационных рисков
- Положение о защите носителей информации
- Положение об обеспечении целостности программно-аппаратной среды объекта КИИ
- Положение о физической защите объекта КИИ и среды ее функционирования
- Положение об управлении персоналом объекта КИИ
- Положение об информировании и обучении персонала по вопросам ОБИ КИИ
- Положение о защите коммуникаций
- Положение по аудиту безопасности информации

Этап ввода в действие

На этапе ввода СОБ ОКИИ в действие осуществляется выполнение мероприятий по ОБИ, предусмотренных техническим проектом:

- Поставка оборудования и программного обеспечения СОБ ОКИИ согласно закупочной спецификации
- Специальная проверка несертифицированных СОИ и СЗИ на предмет обнаружения возможно внедренных в них электронных устройств перехвата информации («закладок»), а также специальные исследования этих средств
- Монтаж оборудования
- Установка и настройка ПО в соответствии с проектными решениями
- Предварительные испытания и ввод СОБ ОКИИ в опытную эксплуатацию
- Опытная эксплуатация СОБ ОКИИ в целях проверки ее работоспособности и отработки технологического процесса обработки (передачи) информации. При необходимости, по результатам опытной эксплуатации СОБ ОКИИ осуществляется ее

доработка
- Приемо-сдаточные испытания СОБ ОКИИ по результатам опытной эксплуатации с оформлением приемо-сдаточного акта, подписываемого разработчиком (поставщиком) и заказчиком
- Аттестация объекта КИИ по требованиям безопасности информации

Заказ услуг

- по телефону: +7 (925) 203-95-11
- по e-mail: info@globaltrust.ru
- через web-форму